

WHAT IS CLAIMED IS:

*See  
a*

005190" 2T546560

- 1 1. A method for securely transmitting data in a network,  
2 said method comprising:  
3 establishing a secure connection between a plurality  
4 of computers and transmitting a password across  
5 the secure connection, the password used to  
6 encrypt and decipher data; and  
7 transmitting data encrypted using the password over a  
8 non-secure connection.
- 1 2. The method as described in claim 1 further comprising:  
2 automatically sending a second password based on an  
3 event, the second password replacing the password  
4 as the encryption key.
- 1 3. The method as described in claim 2 wherein the event  
2 includes a time interval event.
- 1 4. The method as described in claim 2 wherein the event  
2 includes a preset number of transmissions occurring  
3 between two or more computers within the plurality of  
4 computers.
- 1 5. The method as described in claim 1 wherein the network  
2 includes the Internet.
- 1 6. The method as described in claim 1 further comprising:  
2 sending a request from the first computer to the  
3 second computer prior to the establishing of the  
4 secure connection; and

5 responding to the request by the second computer, the  
6 response further includes:  
7 informing the first computer that the second  
8 computer accepts encrypted data.

1 7. The method as described in claim 1 further comprising:  
2 changing the password by including a counter as part  
3 of the password; and  
4 wherein the counter is incremented after each  
5 transmission between the first and second  
6 computer systems.

1 8. The method as described in claim 1 wherein the data is  
2 selectively encrypted.

1 9. The method as described in claim 1 wherein the  
2 selection is based on determining a sensitivity  
3 corresponding to the data.

1 10. The method as described in claim 1 wherein the  
2 deciphering further comprises:  
3 analyzing the data packet and determining whether the  
4 data packet is encrypted; and  
5 selectively deciphering the data packet based on the  
6 analyzing.

1 11. A computer system comprising:  
2 a networked computer system including a plurality of  
3 computers connected by a computer network, each  
4 of the computers including:  
5 one or more processors;  
6 a memory connected to the processors; and  
7 a network connection that connects the computer  
8 with the computer network;

005451 051500

a

a

09594517 "061500

9 and  
10 an encryption tool, the encryption tool including:  
11 means for establishing a secure connection  
12 between a first computer system and a second  
13 computer system, each of the computer  
14 systems connected to a computer network;  
15 means for sending a password from the first  
16 computer system to the second computer  
17 system across the secure connection;  
18 means for encrypting one or more packets of data  
19 using the password as an encryption key;  
20 means for transmitting the one or more packets of  
21 data from one of the computer systems to the  
22 other computer system; and  
23 deciphering the one or more packets of data at  
24 the receiving computer system using the  
25 password as the encryption key.

1 12. The computer system as described in claim 11 wherein  
2 the computer network is a private network.

1 13. The computer system as described in claim 11 wherein  
2 the encryption tool further includes:  
3 means for sending a second password, the second  
4 password replacing the password as the encryption  
5 key.

1 14. The computer system as described in claim 11 wherein  
2 the encryption tool further includes:  
3 means for sending a request from the first computer  
4 system to the second computer system prior to the  
5 establishing of the secure connection; and

6 means for responding to the request by the second  
7 computer system, the response further includes  
8 response data indicating that the second computer  
9 system accepts encrypted data.

1 15. The computer system as described in claim 14 wherein  
2 the means for sending is performed on a defined time  
3 interval.

1 16. The computer system as described in claim 14 wherein  
2 the means for sending is performed after a preset  
3 number of transmissions between the first and second  
4 computer systems.

1 17. The computer system as described in claim 11 wherein  
2 the computer network includes the Internet.

1 18. The computer system as described in claim 11 wherein  
2 the encryption tool further includes:  
3 means for changing the password by including a counter  
4 as part of the password;  
5 wherein the counter is incremented after each  
6 transmission between the first and second  
7 computer systems.

1 19. A computer program product in a computer usable medium  
2 for encrypting data between computers, said computer  
3 program product comprising:  
4 means for establishing a secure connection between a  
5 first computer system and a second computer  
6 system, each of the computer systems connected to  
7 a computer network;

0050517.061500

8 means for sending a password from the first computer  
9 system to the second computer system across the  
10 secure connection;  
11 means for encrypting one or more packets of data using  
12 the password as an encryption key and means for  
13 deciphering the data packets using the password  
14 as the encryption key.

1 20. The computer program product as described in claim 19  
2 further comprising:  
3 means for transmitting the one or more packets of data  
4 from one of the computer systems to the other  
5 computer system; and  
6 means for deciphering the one or more packets of data  
7 at the receiving computer system using the  
8 password as the encryption key.

1 21. The computer program product as described in claim 19  
2 further comprising:  
3 means for sending a second password, the second  
4 password replacing the password as the encryption  
5 key.

1 22. The computer program product as described in claim 19  
2 further comprising:  
3 means for sending a request from the first computer  
4 system to the second computer system prior to the  
5 establishing of the secure connection; and  
6 means for responding to the request by the second  
7 computer system, the response further includes:  
8 means for informing the first computer system  
9 that the second computer system accepts  
10 encrypted data..

0054517-061500

1 23. The computer program product as described in claim 19  
2 further comprising:  
3 means for changing the password by including a counter  
4 as part of the password, wherein the counter is  
5 incremented after each transmission between the  
6 first and second computer systems.

1 24. The computer program product as described in claim 19  
2 wherein the computer network includes a private  
3 network.

1 25. The computer program product as described in claim 19  
2 wherein the means for encrypting further comprises:  
3 means for determining whether the data packets include  
4 sensitive information; and  
5 means for selectively performing the encrypting based  
6 on the determination.

1 26. The computer program product as described in claim 19  
2 wherein the means for deciphering further comprises:  
3 means for analyzing the data packet and determining  
4 whether the data packet is encrypted; and  
5 means for selectively deciphering the data packet  
6 based on the analysis.

1 27. A method for transmitting data securely between  
2 computers, said method comprising:  
3 establishing a secure connection between a first  
4 computer system and a second computer system,  
5 each of the computer systems connected to a  
6 computer network;

[illegible]

a

005790" 2T546560

7 sending a password from the first computer system to  
8 the second computer system across the secure  
9 connection;  
10 encrypting one or more packets of data using the  
11 password as an encryption key and responsively  
12 deciphering the data packets using the password  
13 as the encryption key;  
14 transmitting the one or more packets of data from one  
15 of the computer systems to the other computer  
16 system;  
17 deciphering the one or more packets of data at the  
18 receiving computer system using the password as  
19 the encryption key;  
20 sending a request from the first computer system to  
21 the second computer system prior to the  
22 establishing of the secure connection; and  
23 responding to the request by the second computer  
24 system, the response further including:  
25 informing the first computer system that the  
26 second computer system accepts encrypted  
27 data.